Roteador hotspot para acesso à rede autenticado

O objetivo deste documento é descrever a implementação de um gateway para hotspots Wi-Fi usando Zeroshell. Vamos nos concentrar principalmente sobre a forma de autenticar os usuários (RADIUS, Kerberos 5 e certificados digitais X.509) e no RADIUS contabilidade para o tráfego, tempo e custo das ligações. Ele vai dar uma olhada na possibilidade de obtenção de roteador multi-WAN com balanceamento e failover de conexões de Internet e funcionalidades do Portal Captive.

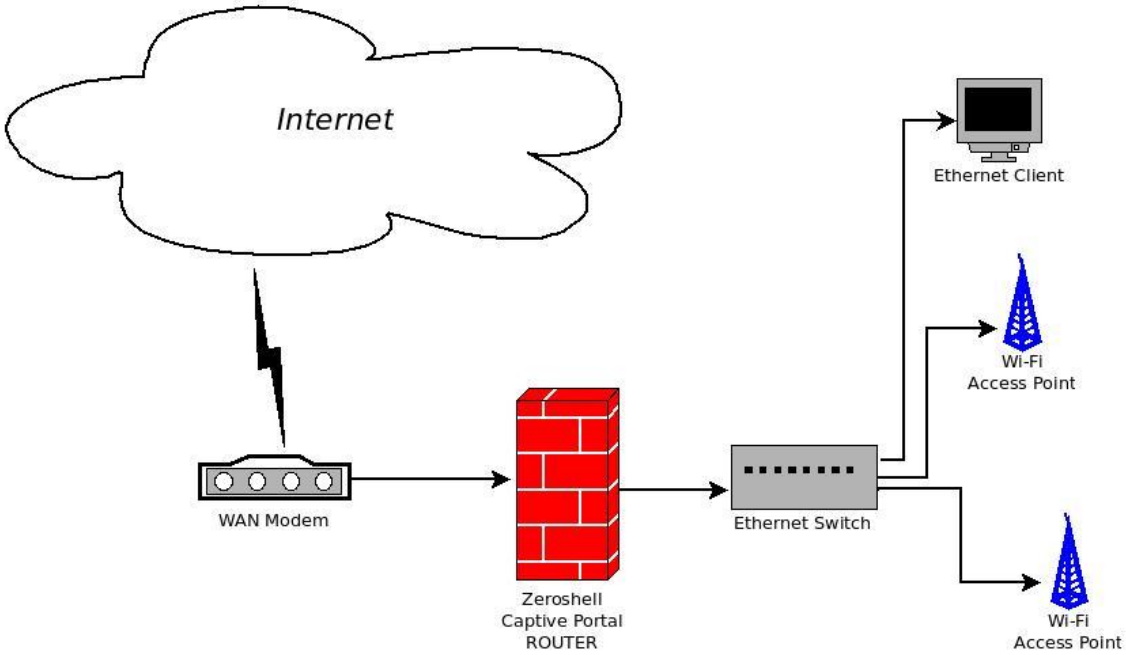


Fig.1 Hotspot rede protegida por um Captive Portal Router

O conteúdo deste documento é subdividido nas seguintes seções:

Introdução

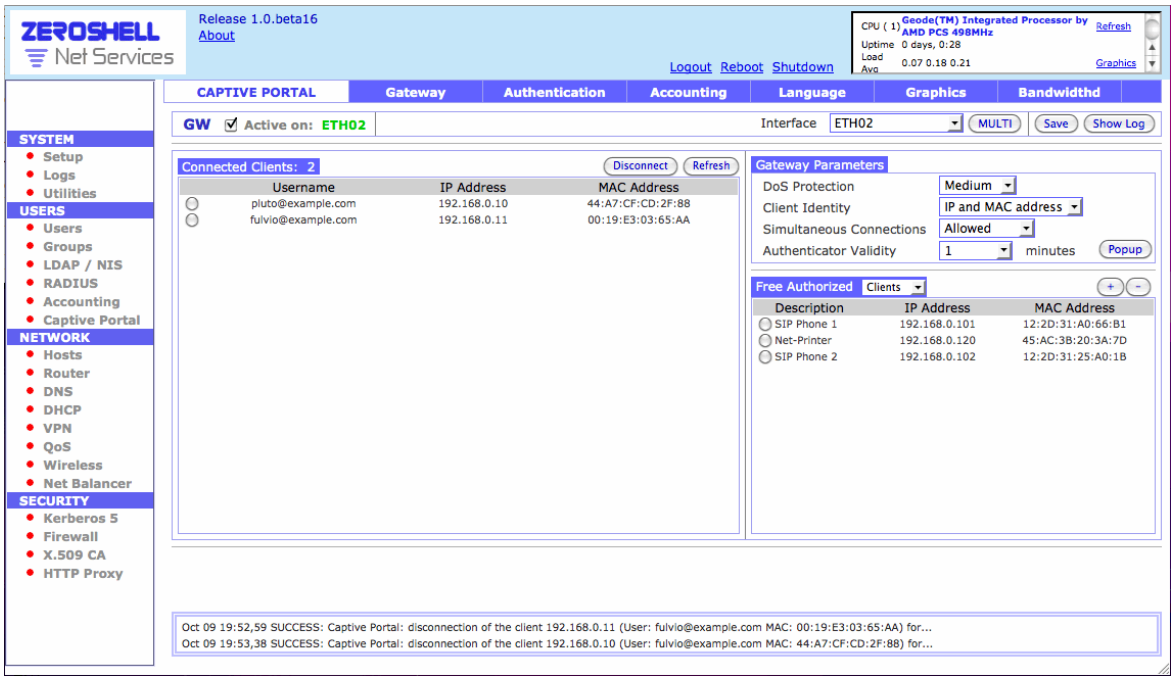
Nos pontos de acesso, que é em lugares públicos onde o acesso à Internet é dada aos utilizadores ocasionais, pelo menos, algumas das seguintes características são necessárias:

1. Autenticação dos usuários
2. Registro dos acessos à rede;
3. Contabilidade para o tráfego, o tempo eo custo das ligações do utilizador.

A autenticação, que é a capacidade de identificar o usuário e, em seguida, conceder acesso à rede, o que pode ser feito através do nome de usuário e senha ou através de um certificado digital X.509 que pode ser armazenado no cartão inteligente.
log O acesso é por vezes necessária por lei, porque nos permite traçar os autores de actividades ilícitas. Lembre-se que o registro não inclui registro de URLs ou pior conteúdo que o usuário tinha acesso, mas simplesmente registrar a data e hora de início e fim de cada uma das ligações à Internet do usuário eo endereço IP associado com o cliente (normalmente um computador portátil), de onde a ligação ocorreu.
representando O, no entanto, para além do controlo do início e fim da ligação, e registará o tempo de trânsito para a ligação de um utilizador. Muitas vezes, o objetivo da contabilidade é o de permitir a cobrança de custos para o tráfego em Megabytes e tempo em minutos de ligação. Além disso, através de contabilidade, você pode definir limites de tráfego e tempo durante o qual o usuário está desconectado da rede. Em particular, a contabilidade pode permitir que o gerenciamento de conexões pré-pagos em que o usuário deve ter um crédito a ser online. Para obter essa funcionalidade você pode usar um ou ambos dos seguintes métodos de acesso:

- Autenticação e criptografia do tráfego via WPA/WPA2 Empresa
- Portal Captive

WPA/WPA2 Empresarial, que requer Wi-Fi Access Points associar um cliente somente se o usuário tem credenciais válidas fiscalizada por um servidor RADIUS usando 802.1x. Além de autenticação, criptografia de tráfego também está garantido entre o cliente eo Access Point.
No caso do acesso via portal cativo em vez disso, os pontos de acesso são programados de modo aberto, isto é, sem qualquer tipo de autenticação e criptografia. O cliente pode associar-se livremente e imediatamente recebe um endereço IP de um servidor DHCP. No entanto, a porta de entrada para o acesso à Internet bloqueando a comunicação com o exterior e redireciona qualquer pedido web (http e https) para uma página de autenticação. Logo fica claro que WPA/WPA2 Enterprise é um sistema mais robusto em termos de segurança em relação ao cativeiro portal, mas, por outro lado, exige que o usuário configure o seu cliente (suplicante) para autenticar via 802.1x. Essa configuração não é fácil para os usuários ocasionais de um ponto de acesso e, por esta razão, que na maioria dos casos, nós preferimos dar acesso usando portal cativo que não requer configuração nos dispositivos móveis.



Captive Portal Configuração do Gateway

Alguns Pontos de Acesso Wireless implementar internamente um portal cativo, mas muitas vezes isso não é configurável e adaptável às necessidades de um hotspot. É mais flexível e conveniente de usar de baixo custo WiFi Pontos de Acesso, sem qualquer recurso avançado e referem-se a função de portal cativo a um roteador que funciona como uma porta de entrada para a Internet, como mostrado na figura 1

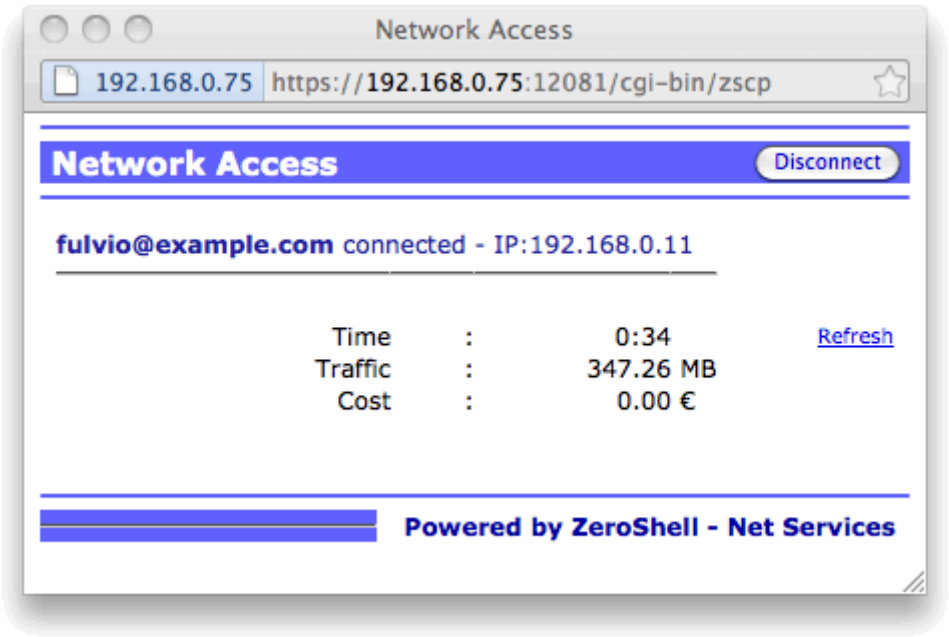
Os inimigos do Portal Captive

A simplicidade no uso de um portal cativo, mesmo por um usuário novato é principalmente devido ao fato de que o acesso ao Nível 2 da rede, se é wireless e rede com fio é aberta (que é não é necessária autenticação). O cliente apenas está associada a rede imediatamente obtém um IP do servidor DHCP e se comunica de uma forma não-criptografada. A contrapartida para essa simplicidade se traduz em uma fraqueza inerente em termos de segurança. Veremos nos próximos dois parágrafos como tentativas Zeroshell para mitigar essa fraqueza.

Spoofing do IP e os endereços MAC

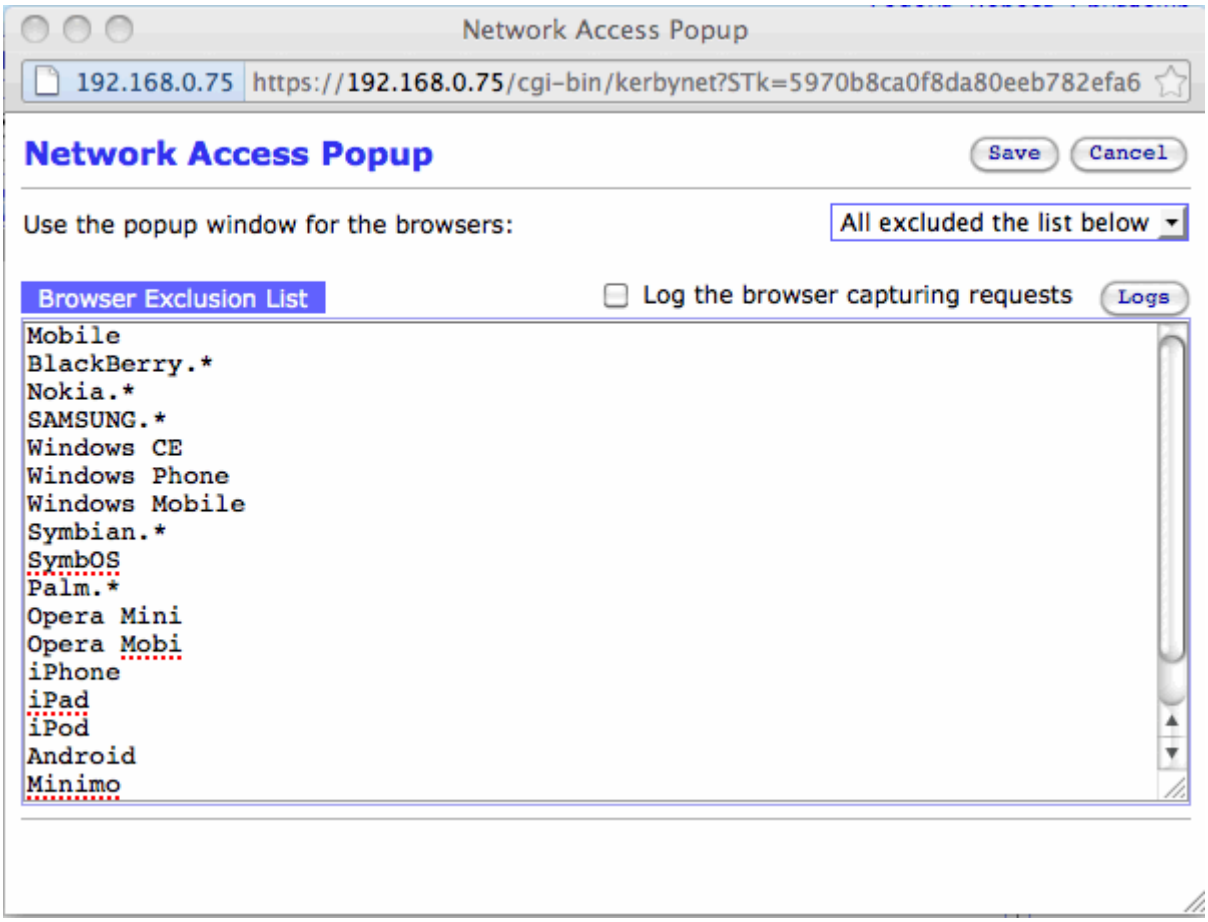
A questão da segurança se sentia ao falar sobre Captive Portal é spoofing os endereços IP e MAC da placa de rede. Na verdade, o firewall do Portal Captive desbloqueia clientes autenticados por identificar os endereços IP e MAC (este último somente se o captive portal está diretamente conectado na camada 2 da rede a ser protegida, que está há nenhum roteador meia). Infelizmente, estes dois parâmetros podem ser ajustados facilmente em qualquer sistema operativo e, por conseguinte, há um risco de que alguém com um sniffer capta o tráfego de olhar para um cliente já autenticado e configurar o mesmo endereço IP e MAC. Isso iria perturbar a comunicação do cliente legitimamente

autenticado que observando a qualidade de conexão baixa, abandona o uso da Internet, deixando espaço para fraudes.
O problema é agravado pelo fato de que a maioria das implementações de portal cativo manter um cliente autenticado conectado até é visível na rede sem que o cliente participar ativamente na renovação de autenticação. Algumas implementações de verificar a tabela ARP, para ver se o cliente tem feito recentemente tráfego ou executar uma solicitação ARP para a verificação da presença da IP na rede. Outros usam a mesa dos arrendamentos do servidor DHCP, verificando se o cliente tenha solicitado a renovação recentemente. Estas soluções são claramente inseguro, porque o cliente tem um papel passivo no recredenciamento de autenticação.
solução de Zeroshell é em vez disso para assegurar que o próprio cliente está a pedir o gateway portal cativo a renovação da autenticação, apresentando um pacote encriptado com AES256, chamado Authenticator. Este é um segredo compartilhado somente pelo cliente e pelo portal cativo (ele viaja no túnel SSL e, portanto, não pode ser capturado com um sniffer), por isso mesmo, se alguém define o IP eo endereço MAC de um usuário autenticado não terá o Authenticator requerida pelo portal cativo para renovar a autenticação. O autenticador é armazenado pelo cliente em uma janela pop-up chamado Popup acesso à rede que lida com o Java Script para enviá-lo para o portal cativo para a renovação.



Janela pop-up de acesso à rede

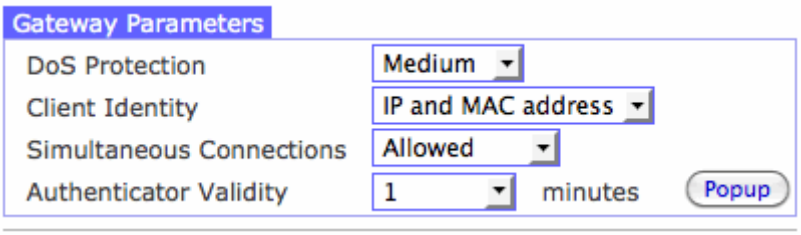
A janela pop-up também executa outras funções, como permitir que o usuário se desconectar e visualizar informações contábeis úteis, tais como o tempo, tráfego e custo da conexão.Deve notar-se que esta janela não é bloqueada por anticorpos anti-up que vem com quase todos os navegador porque é aberto por um pedido síncrono para a autenticação do utilizador. Por outro lado, a janela pop-up tem causado vários problemas com o advento dos dispositivos móveis, como o iPhone, o iPad e outros smartphones e PDAs (incluindo Windows Mobile e Android) que não ter um sistema multitarefa, na verdade, esqueceu-se de renovar a autenticação causando o fecho da ligação. Para solucionar este problema, desde o lançamento 1.0.beta15 de Zeroshell, os dispositivos móveis são reconhecidos pelo portal cativo que não impõe-lhes a renovação de autenticação através do envio do Authenticator, mas simplesmente verificar a sua presença online.



Smartphones e outros dispositivos móveis de configuração

Denial of Service (DoS)

Alguns softwares, em uma tentativa de se comunicar com a rede do lado de fora a qualquer custo, após a tentativa de comunicar nas portas TCP / UDP que lhes forem atribuídas, tente a conexão em portas TCP 80 e 443, sabendo que não é fácil que um administrador de rede iria fechar o tráfego de saída nessas portas que impedem o http / https navegação e, portanto, acessar a web. O exemplo mais conhecido dessa categoria de programas é o cliente de VoIP Skype, mas muitos outros sistemas P2P e vermes têm o mesmo comportamento.Você pode imaginar imediatamente que quando um usuário está associada com seus clientes para a rede, mas ainda não foi autenticado pelo Portal Captive, esses pedidos sobre as portas TCP 80 e 443 será redirecionado para o portal de autenticação que iria tentar, sem sucesso, servir-lhes que o tráfego não é HTTP. É óbvio que mais os clientes não são autenticados ainda e executar esses programas, mais ela aumenta a probabilidade de ocorrência de um DoS (Denial of Service), em que o portal de autenticação está empenhada em servir os pedidos falsos, deixando de operar ou lidar muito lentamente legítimos pedidos de navegadores web.
Zeroshell restringe a ocorrência de tais situações, através da implementação de um sistema de *proteção DoS* usando o Netfilter do Linux para limitar o número máximo de redirecionamentos por minuto. O nível de proteção pode ser definido em três níveis (Baixo, Médio e Alto).



Captive Portal Proteção contra Negação de Serviço

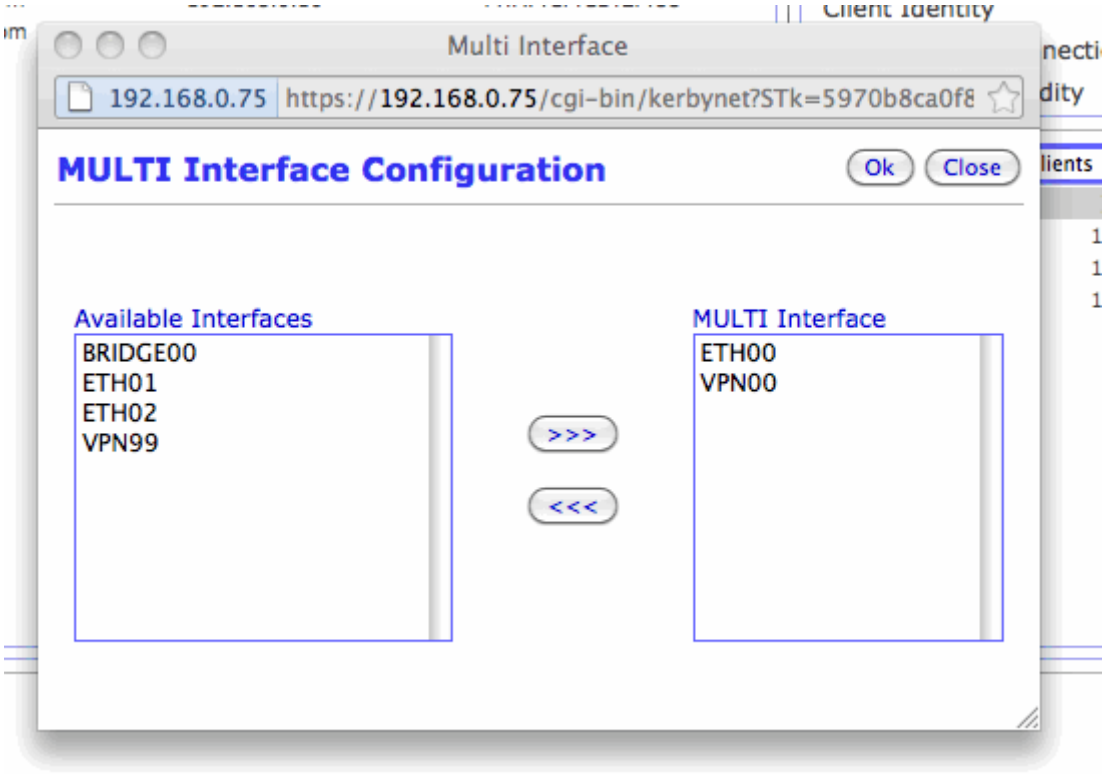
Além disso, os mecanismos de auto-atualização dos sistemas operacionais e das assinaturas de antivírus frequentemente usam o protocolo http para se comunicar com o repositório de atualização e, portanto, pode agravar a situação, fazendo com que as solicitações que são adicionados à carga de trabalho do Portal Captive. Novamente Zeroshell tenta conter o problema, interceptando pedidos para o repositório mais comum evitando desnecessário redirecionamento para a página de autenticação do Captive Portal.

Router ou Bridge?

Na Figura 1 o portal cativo funciona como um roteador 3 Nível ligado directamente a um modem que o liga à Internet. Ele atua como o gateway padrão para clientes que se conectam à rede. Nesta configuração, disse em *modo roteado* , é conveniente que o roteador tem a função de servidores DHCP e DNS. Captive Portal do Zeroshell também pode funcionar em *modo bridge* , onde a rede a ser protegida pelas ações Captive Portal mesma sub-rede IP como o resto da rede. Portanto, o cliente recebe o mesmo endereço IP se você conectar de um lado do que o outro e tem o mesmo gateway padrão que é um roteador antes do Captive Portal. Neste caso, DHCP e DNS para ser usado para o ponto de acesso podem ser os mesmos que os utilizados para o resto da rede. Nas versões anteriores do Zeroshell que tinha a declarar expressamente o modo de operação (Routeadas ou ponte) do portal cativo. Desde o lançamento 1.0.beta15, no entanto, existem duas notícias sobre:

1. Ele é tratado a interface MULTI onde você pode declarar múltiplas interfaces de rede em que para ativar o Portal Captive. Como mostrado na Figura Portal Captive também pode ser habilitado em 802.1q VLAN (Virtual LAN Tagged);
2. Zeroshell seleciona o modo bridge ou roteador verifica automaticamente se ou não uma interface é parte de uma ponte.

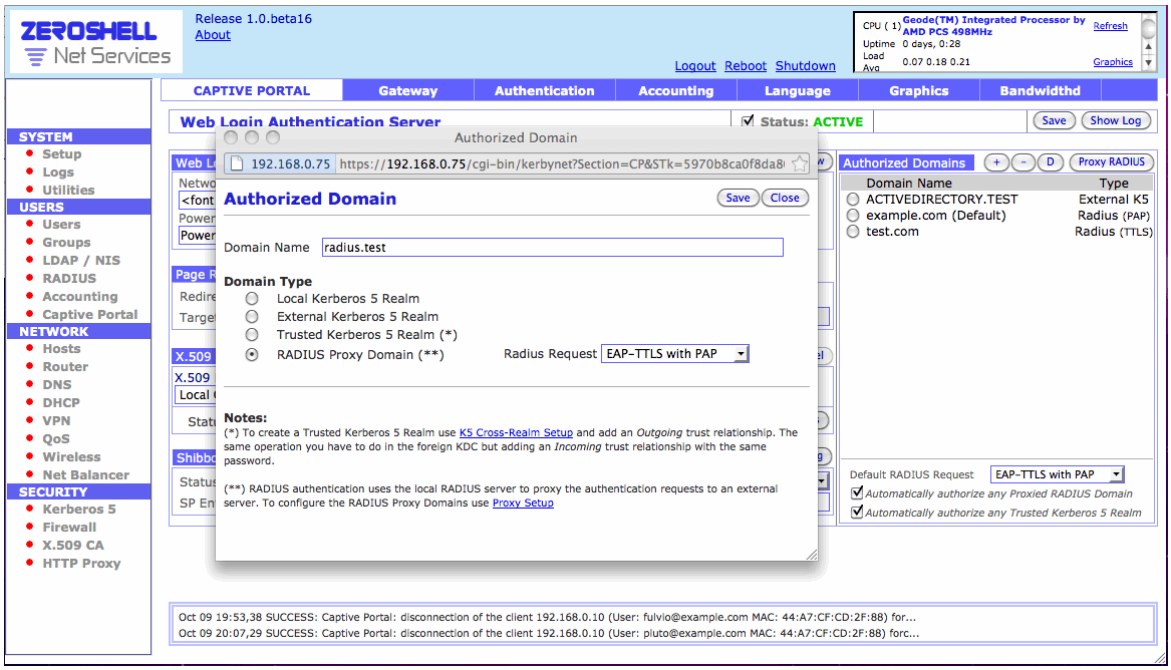
Juntando as duas inovações, se deduz que o Captive Portal de Zeroshell podem trabalhar simultaneamente na mesma caixa de hardware como um roteador para alguns segmentos de LAN e como uma ponte para os outros.



Portal Captive aplicado em múltiplas interfaces de rede

Autenticação de Usuário

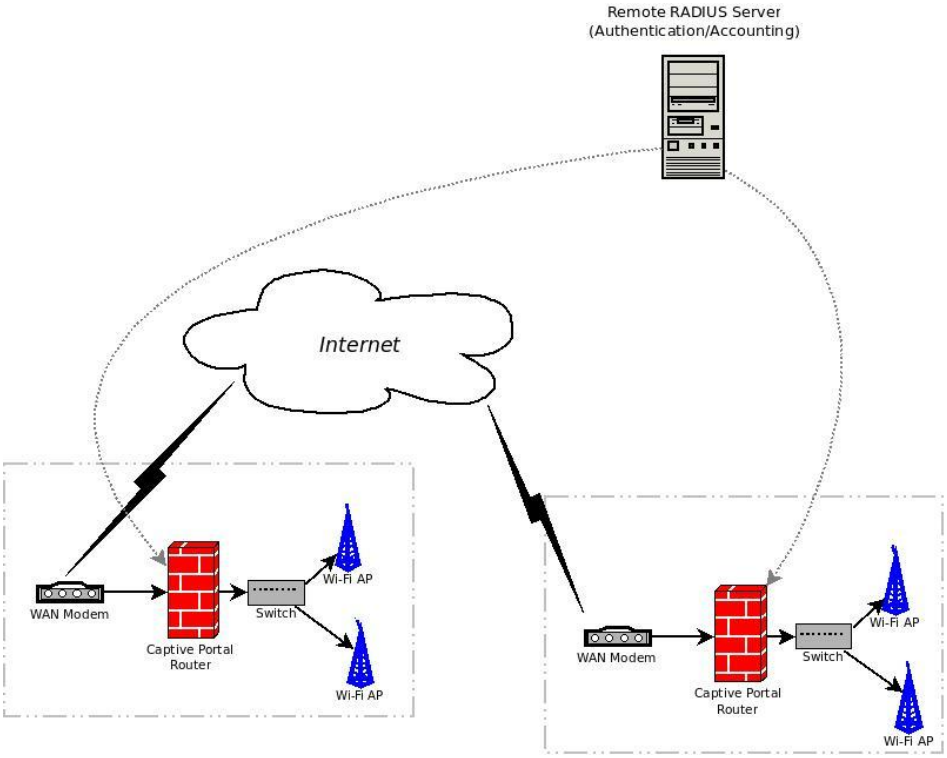
O Portal Captive de Zeroshell pode usar diferentes fontes de autenticação simultaneamente. Por padrão, ele autentica os usuários que utilizam o seu Kerberos 5 KDC que contém princípios para usuários internos armazenados no diretório LDAP e gerenciados através da interface web. No entanto, você pode usar fontes de autenticação externos, tais como Kerberos 5 Realms, servidores RADIUS e provedores de identidade SAML 2. Além disso, há também o de login usando certificados digitais X.509 que permitiria o acesso à rede através de cartão inteligente ou token USB.
No caso de RADIUS ou autenticação Kerberos 5, os usuários podem vir de diferentes domínios. Neste caso, o usuário deve selecionar o domínio de autenticação usando a caixa de seleção na página de acesso ou qualificando o seu nome de usuário usando @ sufixo de domínio (por exemplo pluto@example.com).



Domínios de autenticação autorizado para o hotspot

RADIUS (PAP, EAP-TTLS e PEAP)

Autenticação RADIUS é um dos protocolos mais utilizados para o reconhecimento de usuários em dispositivos de rede, tais como pontos de acesso sem fio ou switches Layer 2 que permitem o acesso ao nível 2 somente após a autenticação foi bem sucedida. O Portal Captive de Zeroshell permite que as solicitações de autenticação RADIUS para servidores externos via proxy. Em outras palavras, o portal cativo requer autenticação para o servidor FreeRADIUS interno, que se descobre que ele não é autoridade para o domínio ao qual o usuário pertence, ele encaminha a solicitação de autenticação para o servidor RADIUS autoridade externa. Claramente, o servidor RADIUS externo deve ser configurado na lista de servidores proxy, especificando o segredo compartilhado. Por outro lado, mesmo no servidor RADIUS externo, uma entrada deve ser adicionado entre os clientes RADIUS para que o endereço IP do Portal Captive usando o mesmo segredo compartilhado. Na lista de proxy RADIUS, você pode adicionar o servidor RADIUS padrão que é usado quando nenhum dos outros servidores está autorizado para autenticar o usuário. O raio de proxy padrão é frequentemente utilizado mesmo quando o portal cativo tem para autenticar contra uma hierarquia de servidor RADIUS.

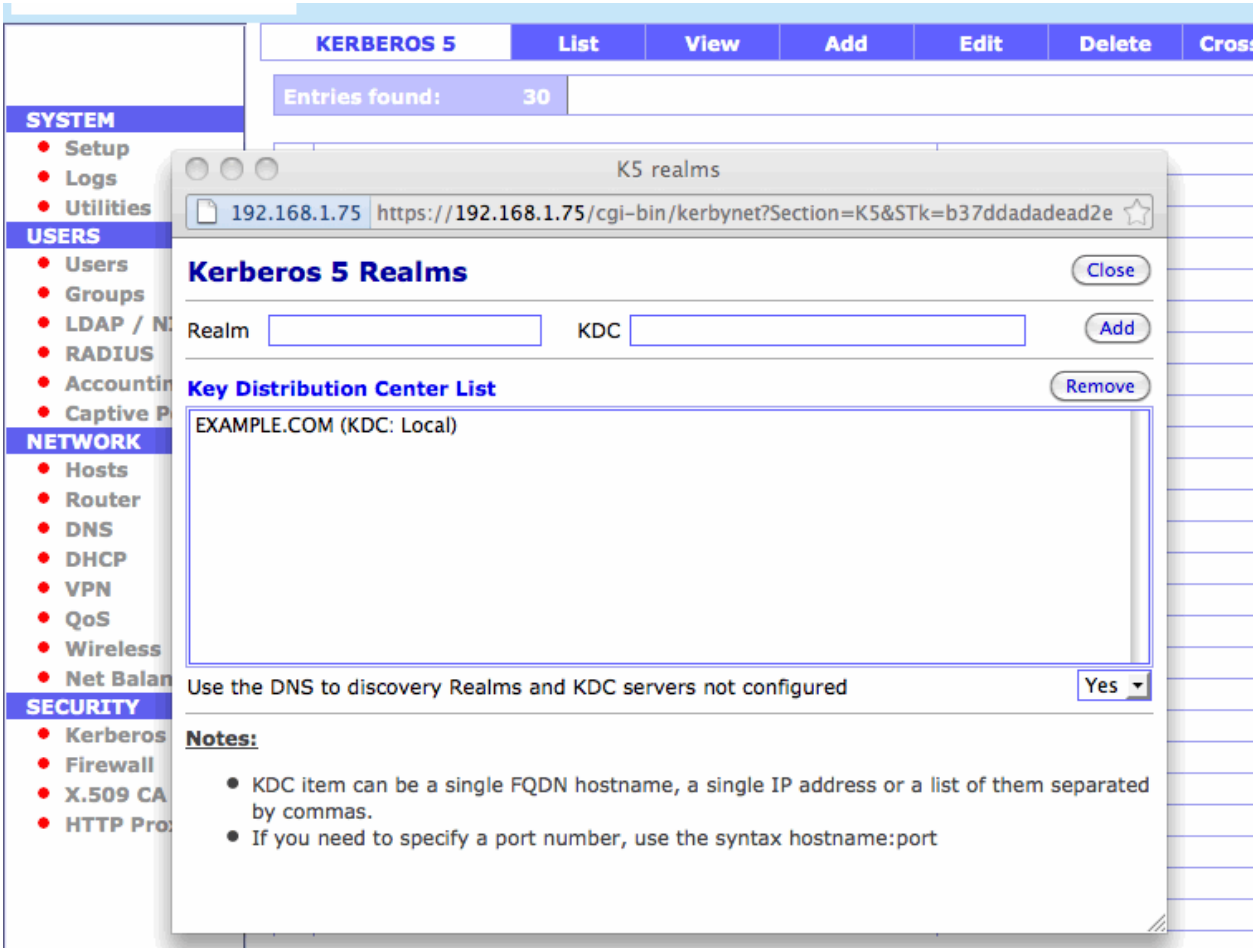


Distribuído Hotspots usando um servidor RADIUS centralizado

O portal cativo pode fazer solicitações de autenticação via PAP ou 802.1x (EAP-TTLS com PAP e PEAP com MSCHAPv2). Neste último caso, o portal cativo aparece para o servidor RADIUS como um suplicante que tenta acessar a rede WiFi via WPA/WPA2 Corporativo. O uso de 802.1x é recomendado durante o PAP simples, se você precisa de um maior nível de segurança, garantida pelo protocolo TLS que EAP-TTLS, PEAP (EAP Protect) use.

Kerberos 5 (Diretório Ativo)

A autenticação Kerberos 5 portal cativo permite que a interface de um domínio do Active Directory do Windows. Na verdade, cada Windows Server que é um controlador de domínio tem a Kerberos 5 KDC que autentica os usuários no domínio do Active Directory ao qual ele pertence. Portanto, basta adicionar o portal cativo autorizado domínios o nome do domínio do Active Directory para permitir que usuários do Windows para acessar a rede. Note que, se a descoberta automática do reino e KDC via registros DNS SRV não está ativo você precisa especificar manualmente os endereços IP (ou nomes de host FQDN) do reino KDC autoritário.



Kerberos configuração de cinco reinos

Em algumas situações, pode ser necessário para permitir o acesso através do portal cativo somente utilizador que pertence a um grupo. Isso não é possível usar Kerberos 5, uma vez que só lida com a autenticação do Active Directory, enquanto autorização é delegada a LDAP. No entanto, você pode ligar os controladores de domínio, o IAS (o serviço RADIUS do Active Directory) e configurar o portal cativo para autenticação RADIUS. Neste caso, você pode configurar o IAS para autorizar apenas os usuários que pertencem a um grupo selecionado.

Certificados digitais X.509 (Smart Cards)

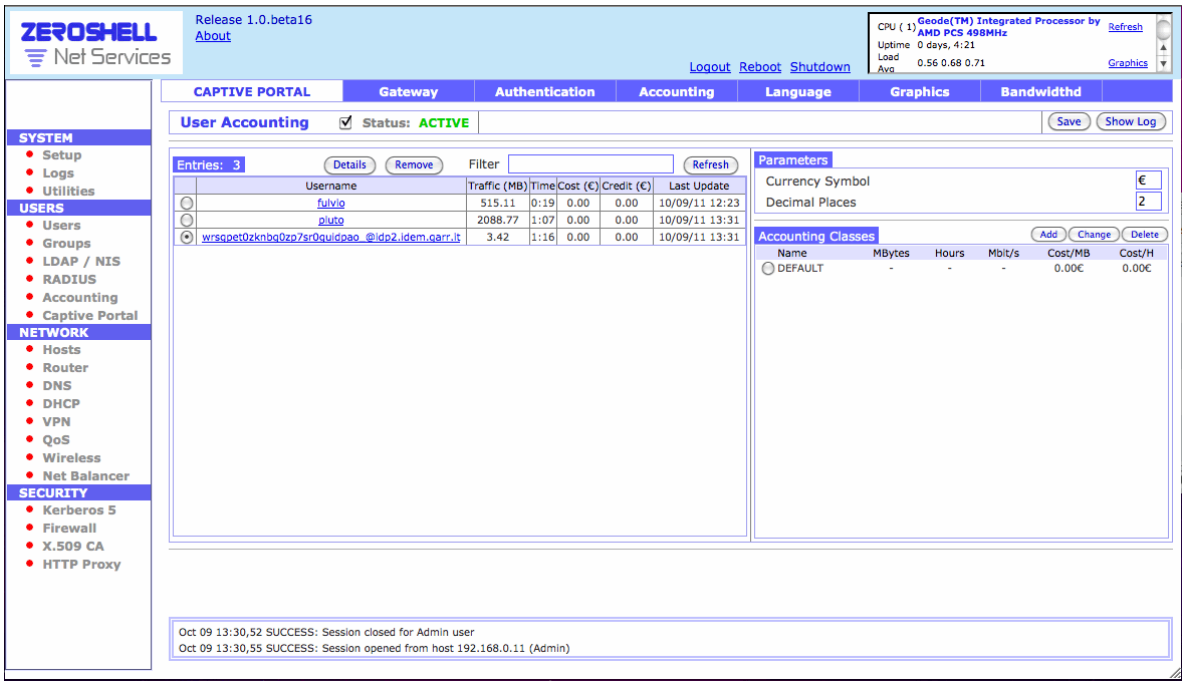
Autenticação via certificados digitais X.509 permitir o acesso à rede sem precisar digitar seu nome de usuário e senha. Em outras palavras, cada usuário que precisa de acesso à rede deve ter um certificado pessoal com sua chave privada carregada no navegador da web. Pressionar o botão [X.509] no portal de autenticação, se o certificado é assinado por uma Autoridade Certificadora habilitada na configuração do portal cativo, o usuário tem acesso à rede. O uso de certificados digitais é muitas vezes relacionada com a dos cartões inteligentes ou tokens USB. Estes dispositivos podem manter o certificado digital de um modo extremamente seguro, porque a chave privada não pode ser extraída com uma operação de leitura a partir do exterior. Os cartões inteligentes são, portanto, equipado com seu próprio chip do processador que realiza a criptografia ea descriptografia pedidos através da API.Para desbloquear a chave privada usada pelo navegador do Smart Card requer a introdução de um PIN, o que ajuda a aumentar a segurança, se o cartão for perdido.

Shibboleth (IDP SAML 2.0)

Usando Shibboleth Service Provider, o Captive Portal de Zeroshell permite a autenticação do usuário contra um provedor de identidade SAML 2. Isto é frequentemente usado nas federações em que cada membro de uma federação implementa um IdP para reconhecer usuários e vários Web Services (Service Provider). Estes serviços podem incluir acesso a uma rede Wi-Fi, no qual o usuário é redirecionado para o WAYF / DS a partir do qual ele / ela seleciona o provedor de identidade oficial para autenticá-lo. Pode-se argumentar que prender o portal cativo para uma hierarquia de servidores RADIUS (como eduroam no que diz respeito às universidades e instituições de pesquisa), seria no entanto um acesso federado para a rede. No entanto, enquanto que no caso de 802.1x o chamado *ponto-a-fim* de autenticação tem lugar também atravessar a hierarquia de servidores RADIUS, com o portal cativo que não é garantida. Portanto, é preferível usar SAML, onde em vez, as credenciais de viagens, a partir do navegador do usuário para seu IdP autoritário, sempre dentro do mesmo túnel SSL criptografado, garantindo a autenticação end-to-end. Mais detalhes sobre o Portal Captive Shibboleth estão disponíveis no documento Configure o Captive Portal para autenticar os usuários contra um IdP SAML 2.0 usando Shibboleth .

Contabilizar o tempo, o tráfego e custo das ligações

A contabilidade nos permite conhecer, para cada usuário, o tempo, o tráfego eo custo das conexões. O Portal Captive de Zeroshell usa o protocolo RADIUS para transmitir tais informações, assim você pode usar um servidor externo que suporta o RADIUS contabilidade ou apenas módulo de contabilidade dentro Zeroshell baseado em FreeRADIUS. Como a autenticação, também a contabilidade pode ser centralizada em um único servidor RADIUS que recolhe informações de várias hotspots. Além disso, mantenha em mente que o sistema de contabilidade de Zeroshell pode, porque ele atende o padrão RADIUS, coletar informações também directamente a partir do ponto de acesso Wi-Fi que usam WPA/WAP2 empresa com 802.1x.



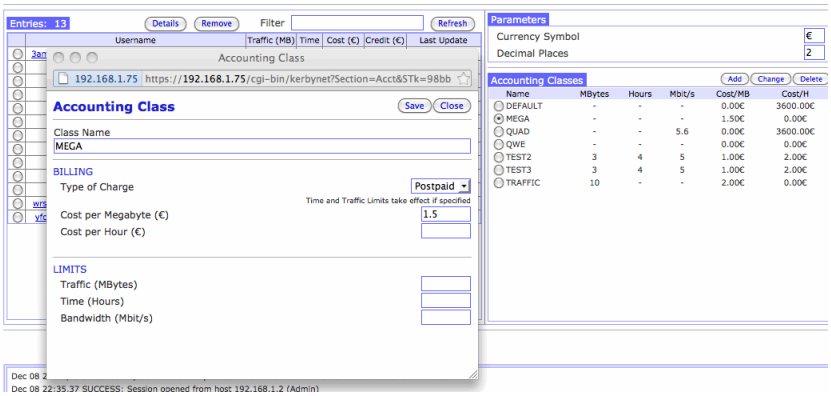
Informações Accountig RADIUS

Detalhes da contabilidade do usuário

Limites de acesso à rede

Usando contabilidade RADIUS, é possível também definir limites de conexão para os usuários. Para isso, basta atribuir os usuários a uma classe de contabilidade para que você dê os seguintes parâmetros:

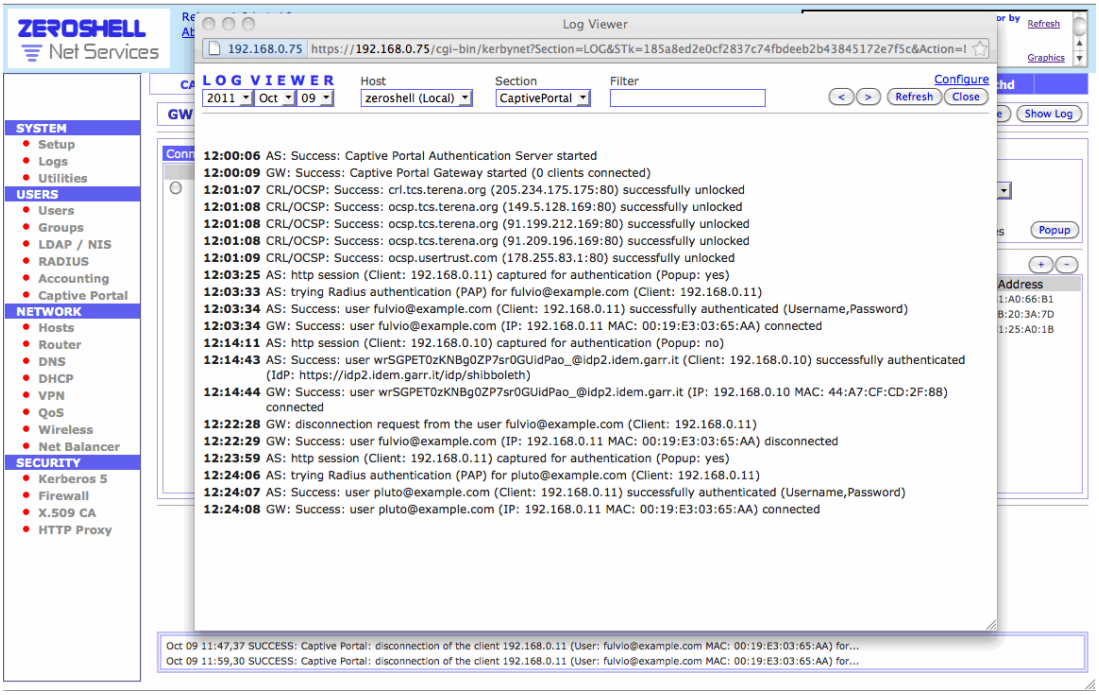
- Tipo de pagamento (pré-pago e pós-pago)
- Custo por megabyte de tráfego
- Custo por hora de conexão
- Limite máximo de tráfego (entrada e saída), em Megabytes
- Limite de tempo de conexão



Limites de configuração do usuário na contabilidade

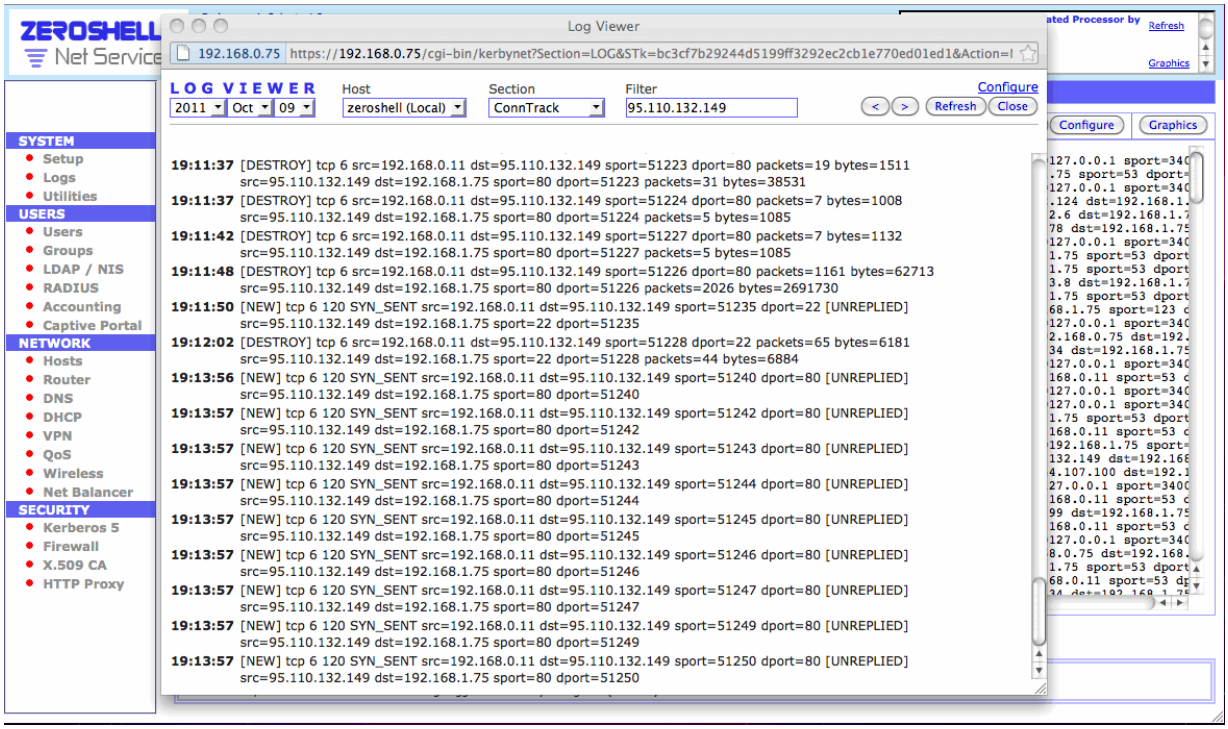
Registro de acessos de usuários e conexões TCP / UDP

Embora já a contabilidade mantém o controle de conexões de usuários à rede, é possível ter mais detalhes sobre a autenticação do usuário, olhando para as mensagens de log referentes ao Portal Captive.



Mensagens de log do Portal Captive

Além disso, especialmente se os clientes do portal cativo usando endereços IP privados, pode ser útil para manter o controle de conexões TCP e UDP que são estabelecidas com servidores externos, uma vez que o portal cativo deve executar NAT (Network Address Translation), todas as conexões aparecem gerado pelo IP público do router. O registro do acompanhamento de conexões devem ser explicitamente habilitado e recomenda-se avaliar, antes de ativá-lo, que o seu uso é permitido pelas leis de privacidade, tendo em conta o fato de que ele não pode ser usado para saber o conteúdo de usuários ' comunicação, mas apenas para determinar os servidores que foram contactados.



Rastreamento de ligação das conexões TCP / UDP

O balanceamento de carga e tolerância a falhas das conexões à Internet

Para garantir a largura de banda adequada e estável para Internet pode permitir balanceamento de carga e tolerância a falhas para links WAN. Zeroshell pode funcionar em dois modos chamados *de failover e balanceamento de carga* e *failover* . No primeiro caso, todo o tráfego é encaminhado pelo elo mais eficiente, enquanto outras conexões são peças de reposição e só pode ter lugar em caso de falha do ativo. No balanceamento de carga e modo Failover, em vez disso, todas as ligações são simultaneamente ativos eo tráfego é encaminhado por eles em round-robin. Mesmo neste último caso, é garantida a tolerância a falhas, uma vez que, se uma ligação é inacessível é automaticamente excluídos do equilíbrio até que ele retorne acessível.
Além disso, é possível equilibrar o tráfego manualmente. Por exemplo, você pode decidir que o tráfego VoIP é encaminhado por um link, enquanto que a gerada pela transferência

de arquivos de um outro. Isso irá evitar a saturação do link que iria produzir ruído na comunicação VoIP. Para mais detalhes, leia o documento várias ligações à Internet através de um equilíbrio de tráfego e gerenciamento de Failover .

Traduzido e enviado por : Carlos Daniel Silva