NetScreen 5XT na tapetě

> VLADIMÍR KOTAL, VÁCLAV PETŘÍČEK, JAKUB YAGHOB

Rostoucí počet útoků po síti a na druhé straně pak požadavků na jejich co nejlepší zabezpečení znamená konjunkturu pro dodavatele firewallů. Jedním z nich je produkt NetScreen 5XT firmy NetScreen Technologies Inc. sídlící v blízkosti San Francisca v USA, jehož výhradním distributorem v ČR je společnost VUMS-Datacom. Následující text podrobně rozebírá vlastnosti, instalaci a užívání tohoto hardwarového firewallu.

Vlastnosti podle dokumentace

V nabídce firmy NetScreen je to jeden ze slabších produktů. Jde se ovšem o firewall, vhodný především pro zabezpečení malých firem či jednotlivých kanceláří. Tomu také odpovídají parametry uvedené v ***tabulce 1.***

Vestavěný ScreenOS je stavovým firewallem se solidním počtem módů funkčnosti a odolným proti řadě útoků:

> konfigurovatelná ochrana pro každé rozhraní, včetně SYN útoku, ICMP floodu, port scanu a mnoha dalších (podrobněji na straně 34 Volume 2 dokumentace)
> překlad adres (NAT) a překlad portů (PAT) pro odstínění vnitřních adres
> transparentní mód, kde zařízení funguje jako bridge s firewallem, VPN a ochranou proti DoS s minimální změnou stávající konfigurace
> mód routeru vhodný pro sítě, kde není třeba překládat adresy
> operační systém firewallu ScreenOS je certifikován Common criteria úroveň EAL2 a má také ICSA certifikát
> jako další ochrany jsou uváděny ochrany proti DoS a DDoS, útoku fragmentovanými TCP pakety, špatně formovaným paketům a špatně formovaným URL

Parametry NetScreen 5XT

Počet rozhraní	1 nedůvěryhodné (před firewallem) 4 bezpečné (za firewallem)
Rychlost a druh rozhraní	10/100 Ethernet
Další rozhraní	modemový port a konzolový port
Maximální přenosová rychlost	70Mbps pro firewall a 20Mbps pro VPN s 3DES
Maximální počet IP adres na bezpečné straně	neomezeno
Maximální počet sessions (aktivních spojení)	2000
Maximální počet VPN tunelů	10
Maximální počet bezpečnostních pravidel	100
Maximální počet bezpečnostních zón	2
Maximální počet virtuálních routerů	2
Podporované routovací protokoly	RIP v.2, OSPF, BGP

> Výrobce nabízí tento firewall ve dvou konfiguracích. Jedná se o konfiguraci základní, která omezuje počet konkurentních uživatelů na 10, a to při ceně USD 495, a konfiguraci Elite, která počet konkurentních uživatelů neomezuje, za cenu USD99.

Obsah dodávky

V krabici najdete samotný firewall, který je poměrně malý a lehký (a tedy vhodný i domů nebo malých kanceláří), zdroj, dokumentaci na CD a ethernetové kabely. A co se schovává uvnitř? Neodolali jsme a firewall rozebrali. Uvnitř se nachází procesor PowerPC 405GP a zcela jistě také zaujme Gigascreen B0 ASIC, který plní hardwarové úkoly firewallu.

Dokumentace na dodávaném CD je

psaná srozumitelně a je i dostatečně obsáhlá. Nicméně některé obrázky jsou příliš komplikované a členité.

Instalace a užívání

Pro první připojení a konfiguraci firewallu je možno zvolit několik přístupů:

> terminálové rozhraní přes konzolový port (přesné hodnoty nastavení jsou v dokumentaci)

> webové rozhraní přes ethernet na důvěryhodné straně firewallu (má adresu 192.168.1.1) pomocí protokolů HTTP nebo HTTPS

> přístup přes další protokoly – SSHv1, Telnet, Netscreen Global Administration (proprietární protokol firmy NetScreen)

> Firewall NetScreen 5XT byl testován ve spolupráci Network Computingu a katedry softwarového inženýrství Matematicko-fyzikální fakulty UK v Praze. K testování jej zapůjčila společnost VUMS-DataCom.

Připojení přes ethernet proběhlo hladce, připojení přes konzolový port potřebuje nullmodemový kabel, který však není součástí dodávky.

Při obou druzích přístupu je ovšem vhodné změnit přístupové heslo. Počáteční nastavení je netscreen/netscreen. Při nastavování nového hesla je administrátor důrazně varován, že nelze zpětně zjistit heslo při jeho ztrátě. Pokud tato situace přece jen nastane, nezbývá než použít jednu ze dvou možných metod pro znovunastavení přístupového hesla. Obě tyto metody pracují pouze v konzolovém režimu.

Po počátečním nastavení lze nastavit i možnosti administrace z ostatních rozhraní firewallu.

Terminálové rozhraní

Využívá tzv. CLI (Command Line Interface) a je vhodnější spíše pro zkušené síťové administrátory. Zde administrátor pomocí CLI nastaví, příp. zjistí všechny potřebné parametry firewallu.

CLI je velmi podobná IOS firmy Cisco, bohužel se však v některých případech liší (např. přejmenované příkazy, konfigurace není hierarchická), což přináší potíže právě zkušeným síťovým administrátorům, kteří obvykle s prvky firmy Cisco pracují.

WebUI

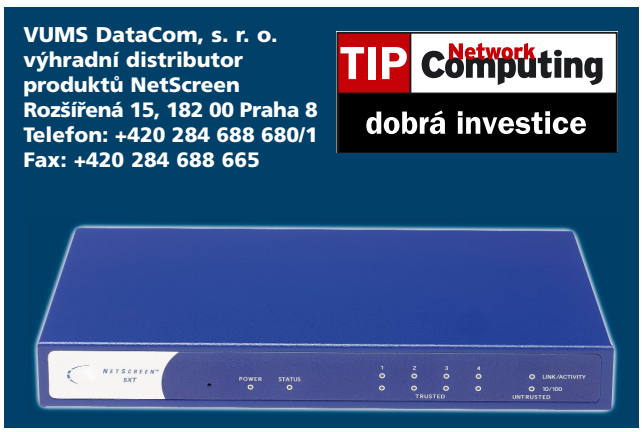
Druhou možností přístupu je přístup přes webové rozhraní, které je zde případně nazýváno WebUI. Tato možnost je vhodnější spíše pro méně zkušené administrátory. Vše je zde řešeno pomocí tzv. wizardů, které administrátora vedou jednotlivými kroky.

K dispozici jsou instalační wizard (spouští se sám při prvním přístupu), wizardy pro nastavení příchozí a odchozí bezpečnostní politiky a wizard pro nastavení VPN.

Jako velmi dobrá se jeví nápověda, kterou lze vyvolat pro každou podsekci konfigurace, a odkaz vede na webovou stránku firmy NetScreen s detailním popisem konfiguračních elementů dané podsekce.

VPN

Pro vytváření VPN je docela vhodné použít wizard z WebUI i pro zkušeného administrátora. Zde je nutno nastavit pravidla politiky pro VPN, gateway a IKE/pevných SPI (Security Parameter Index). Informace jsou na sebe hierarchicky vázány a nelze smazat pravidla politiky bez zrušení nastavení IKE a gateway, což může v některých případech být i nevýhoda. Problém nastal při změnách parametrů VPN, kdy se nově nastavené parametry neuložily (toto platí pro WebUI).



Notifikace

NetScreen má poměrně rozsáhlé možnosti informovat správce o svých stavech. Jednou z možností je e-mail, kde jsou zasílány části logů při dané události. Další možností je už tradiční SNMP, kde NetScreen zasílá SNMP trapy. To je vhodné do prostředí, kde již existují prostředky pro sledování sítě. K dispozici jsou ještě syslog, webtrends a NetScreen Global Pro (proprietární protokol pro správu většího počtu zařízení firmy NetScreen).

Konfigurace sítě

Konfigurace sítě je opět hierarchická. Nastavují se bezpečnostní zóny, rozhraní a jejich přiřazení do bezpečnostních zón, nastavení IP adresy rozhraní, protokoly administrace na rozhraní, zda jde o NAT nebo routování, lze nastavit šířku pásma rozhraní, ale nic víc (žádná podpora disciplín pro řazení paketů do prioritních front apod.).

Virtuální routery

NetScreen má implicitně dva virtuální routery (VR): důvěry-

hodný a nedůvěryhodný. Přednastaveně jsou všechny spoje přiřazeny do důvěryhodného. Každý VR může mít přiřazeny mapy spojení pro dynamické routování, přístupové seznamy pro import/export routovacích záznamů z dané mapy spojení. To přináší nezanedbatelnou výhodu: můžeme operovat s několika VR, každý z nich má jiné nastavení pro routovací protokoly a jiné routovací tabulky. Tím lze dosáhnout odseparování vnitřní sítě.

ZAŘÍZENÍ:

NetScreen-5XT
Cena: 795 USD za desítiuživatelskou verzi
Cena: 1500 USD za verzi bez omezení počtu připojených uživatelů

Bezpečnostní zóny a politika

Zóny představují v konfiguraci ScreenOS velmi důležitý prvek: pomocí nich se definuje rozdělení sítí na části s různými bezpečnostními možnostmi.
Bezpečnostní politiku pak definujeme jako množinu pravidel, ve kterých figurují zóny. Tak lze např. nastavit, že zóna „finanční oddělení“ bude moci přistupovat do zóny „Mail/POP3“, která je za routerem, ale již nebude moci přistupovat do zóny „Untrust“, která představuje iInternet.

Další součástí nastavení politiky je i určení, zda má být provoz šifrován.
Je možné zvolit i jemnější granularitu, např. oprávnění jenom určitým adresám z dané zóny přístup do dané podsítě jiné zóny, což je podporováno jakýmsi adresářem, ve kterém je uložena část kontextu konfigurace, takže nemusíme znovu vyplňovat podsítě a adresy pro podobná pravidla.
Platí, že jedna zóna může mít přiřazeno více rozhraní NetScreenu, ale jedno rozhraní nelze přiřadit do více zón.
Bezpečnostní pravidla mohou být navíc vázána na určitý časový interval.

Výkon a ochrana

Pro pochopení fungování ochrany je dobré vědět, jak paket prochází zařízením. Pro tento popis by byla nejspíše vhodná ilustrace. Jenže právě tento obrázek je v dokumentaci jedním z těch velmi komplikovaných a nepřehledných. Proto jsme se rozhodli průchod popsat slovně:

1. Paket přijde na rozhraní – paketu je přiřazena bezpečnostní zóna podle toho, zda se jedná o paket ze sítě nebo VPN (tomu se přiřadí bezpečnost ní zóna tunelu).
2. Vyhledání session – ScreenOS si udržuje tabulku sessions, ve které si soustřeďuje informace o zdrojové/cílové adrese, času, rozhraní, atd. Pokud se příchozí paket shoduje se záznamem v tabulce, přeskočí se zpracování všech následujících kroků a paket je předán dál.
3. Překlad MIP (Mapped IP)/VIP (Virtual IP) -> host IP – routovací tabulka už hledá přeloženou adresu.
4. Hledání v routovací tabulce – zároveň přiřadí cílovou bezpečnostní zónu.
5. Hledání politiky – rozhodne o tom, co se stane s paketem. Možnosti jsou tři: povolit, zahodit, tunelovat pomocí VPN.
6. NAT – pokud je zapnutý, změní zdrojovou adresu.
7. Vytvoření session

Jako jedna z ochran je uváděna ochrana před špatně formovanými URL, což je zajištěno filtrováním HTTP provozu pomocí Websense serveru. Ten jsme bohužel neměli k dispozici, proto jsme nemohli tuto část ochrany vyzkoušet.
Také další z ochran vyžadují pro plnohodnotné otestování vytvoření poměrně komplikovaných podmínek (např. DDoS), které by jistě šlo splnit, avšak za cenu zvýšeného nebezpečí nebo zcela neetického chování (např. vypuštění vhodného testovacího „neškodného“ viru pro otestování ochrany před DDoS).

Proto jsme nakonec přistoupili alespoň k jednoduchému testu, který vyzkoušel jak výkon, tak schopnosti obrany firewallu:
Pomocí ICMP floodu z počítače na jednom rozhraní (100base-TX full-duplex) se ukazatel „Sessions“ na WebUI v „Resource status“ tabulce dostal do žlutého pole. Po ukončení floodu velmi rychle (asi 3 vteřiny) klesl na minimální hodnotu.
Pokud se pro danou zónu nastaví ochrana proti ICMP floodu, ukazatel zůstane v zeleném poli, takže minimálně tato ochrana pracuje.

SHRNUTÍ

Tento firewall je jako samostatný prvek vhodný pouze pro malé kanceláře v rozsahu 10-25 zaměstnanců. V takovém případě je ovšem nutné zakoupit verzi Elite, která neomezí počet uživatelů na 10. Pro střední a větší podniky lze pak tento prvek použít jako firewall samostatného malého pracoviště připojeného VPN ke svému kmenovému pracovišti.

Autoři, UNIX System administrator' v COL ***RNDr. Vladimír Kotal, RNDr. Václav Petříček a RNDr. Jakub Yaghob*** *se při testu sešli na Katedře softwarového inženýrství MFF UK. Své názory jim můžete sdělit e-mailem na adresy* ***vlada@devnull.cz (vladya@openbsd.cz); vaclav.petricek@mff.cuni.cz a Jakub.Yaghob@mff.cuni.cz.***