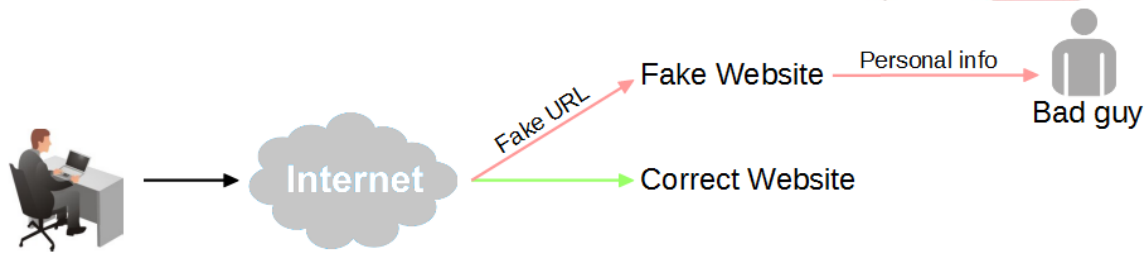
Potansiyel Punycode Phishing Saldırısını Önleyin

Domain Name sistemi, başlangıçta yalnızca sınırlı ASCII karakterlerini kullanacak şekilde tasarlanmıştır. URL'de Unicode karakterleri (diğer dillerin harflerini kapsayan) göstermek için, Punycode sözdizimi kullanılır.

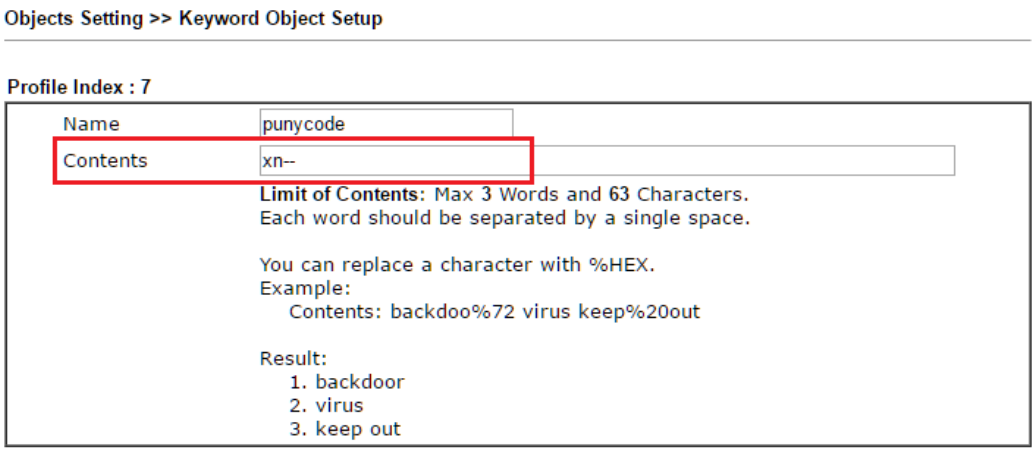
Ancak, URL'lerde Unicode karakterlere izin vermek bazı güvenlik sorunlarına neden olabilir. Tüm yabancı karakterleri kullanabilmek için 'hackerler', kullanıcıların kişisel bilgilerini açıklayabilecekleri iyi bilinen bir web sitesine benzeyen, domaini olan sahte bir web sitesi oluşturabilirler.

Neyse ki, kullanıcıların sahte web sitelerine gitmelerini önlemek için alabileceğimiz basit bir yöntem var. URL, Punycode kullandığını bildirmek için "xn--" ile başlayacaktır, böylece "xn--" içeren URL'leri engellemek için URL Content Filter ve DNS Filteri ayarlayabiliriz.

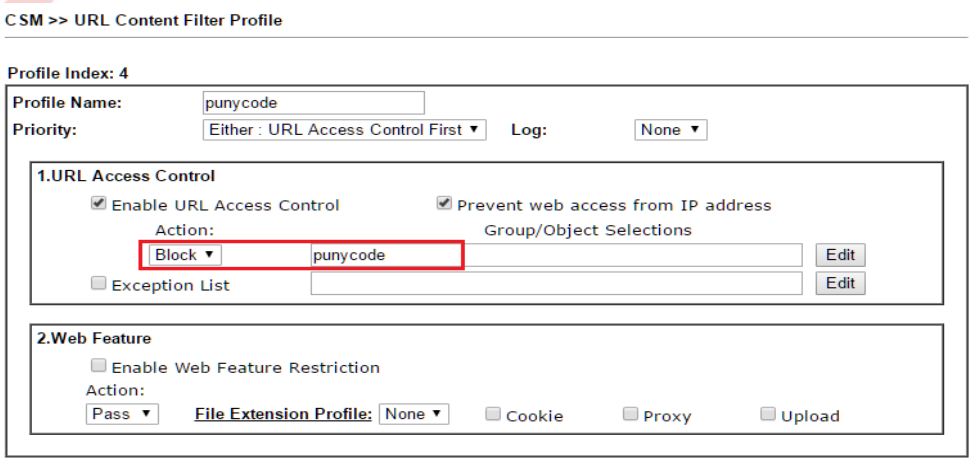


Punycode URL'lerini kullanarak web sitelerini engellemek için:

1. "xn--" içerikli bir Keyword Object oluşturun.



2. Step 1'de belirlediğimiz Keyword'u içeren URL'yi engellemek için bir URL Content Filter profili oluşturun.



3. Step 2'de belirlediğimiz URL Content Filterin DNS isteğini filtrelemek için bir DNS Filter profili oluşturun.

CSM >> DNS Filter

Index No. 4

Profile Name	punycode
Syslog	None
WCF	None
UCF	UCF-4 punycode

4. Step 2 ve 3'de belirlediğimiz kuralları uygulamak için bir Firewall Rule profili oluşturun.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 6

Check to enable the Filter Rule		
Comments	punycode	
Index(1-15) in Schedule Setup	, , ,	
Clear sessions when schedule ON	Enable	
Direction	LAN/DMZ/RT/VPN -> WAN	
Source IP	Any Edit	
Destination IP	Any Edit	
Service Type	Any Edit	
Fragments	Don't Care	
Application	**Action/Profile**	**Syslog**
Filter	Pass Immediately	
Branch to Other Filter Set	None	
Sessions Control	0 / 60000	
MAC Bind IP	Non-Strict	
Quality of Service	None	
User Management	None	
APP Enforcement	None	
URL Content Filter	4-punycode	
Web Content Filter	None	
DNS Filter	4-punycode	
Advance Setting	Edit	